REMARKS

Claims 82-116 remain in this application. Claim 81 has been canceled without prejudice. Claim 82, previously dependent from cancelled claim 81, has been rewritten in independent form. In view of the foregoing amendments, and remarks that follow, Applicant requests favorable considerable and timely indication of allowance.

Claim Rejections

Claim 81 has been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg (U.S. 6,240,091) in view of Schneier. Claims 82-102 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier as applied to claim 81, and further in view of Walker (U.S. 6,263,438). Claims 103-116 have been rejected under 35 USC § 103(a) as allegedly being unpatentable over Ginzboorg in view of Schneier and Walker as applied to claim 81, and further in view of Thompson (U.S. 6,282,552). The rejections of claims 82-116 are respectfully traversed.

Applicant discloses a novel and unobvious cryptographic system for secure communications between a member and a service provider without the need for a trusted third party, such as a public key depository. In one embodiment of the cryptographic system, the member initiates communications by sending a key exchange request message to the service provider. The key exchange request message includes the member's public key, and may be encrypted, at least in part, by the service provider's public key stored on an electronic or smart card of the member. The service provider, in response to the key exchange request message, may generate a session key to be used to conduct a transaction between the two.

According to the Patent Office, Ginzboorg discloses a user terminal that can gain access to a network with a smart card that includes the public key of a charging server, but admittedly does not disclose Applicant's methodology for encrypted communications. Instead, the Patent Office relies on Walker to show the transmission of the user's public key to the charging server, and Schneier's Woo-Lam protocol for disclosing a system using public keys for authentication and a session key for conducting the transaction. Recognizing that the Woo-Lam protocol uses a trusted third party to generate the session key, the Patent Office applies a separate and distinct Encrypted Key Protocol disclosed in Schneier to show that the charging server in Ginzboorg can generate the session key. According to the Patent Office, it would have been obvious to combine the teachings of these two separate and distinct protocols in Schneier, modified by Walker, in the

system disclosed by Ginzboorg in order to achieve the novel and unobvious approach claimed by Applicant.

The position taken by the Patent Office fails for at least two reasons. First, there is no teaching or suggestion in the prior art to support the combination of references. Second, even if one were to attempt to combine these references, as proposed by the Patent Office, the resultant combination would still not yield the claimed invention.

A.   *The Prior Art Does Not Suggest the Desirability of the Claimed Invention.*

A *prima facie* case of obviousness cannot be established unless there is some suggestion in the prior art to motivate the skilled artisan to modify a reference or to combine references. The mere fact that the references **can** be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Fritch*, 972 F.2d 1260, 23 USPQ2d 1780 (Fed. Cir. 1992).

Woo-Lam is directed to a protocol that allows two members on a network to communicate securely using a trusted third party to generate a session key. The Patent Office suggests that one skilled in the art would be motivated to move the session key generation function from the trusted third party to one of the two members to minimize the probability that the session key will be intercepted during transmission and protect against the possibility that the trusted third party is not actually trustworthy. The Patent Office fails to cite any evidence in the record for this proposition, but rather relies on a highly debatable line of reasoning. As noted by the Court in *In re Ahlert*, 424 F.2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970), the notice of fact beyond the record which may be taken by the Patent Office must be "capable of such instant and unquestionable demonstration as to defy dispute." (citing *In re Knapp Monarch Co.*, 296 F.2d 230, 132 USPQ 6 (CCPA 1961)). The Patent Office has failed to meet this standard.

Moreover, the Patent's Office's reliance on facts outside the record, whether true or not, is irrelevant. The Woo-Lam protocol was created specifically to support secured communications between two unknown parties over a network using a trusted third party. The use of a trusted third party is not part of the protocol, but rather an underlying assumption or condition on which the protocol is based. If you change the underlying conditions, then the Woo-Lam protocol is no longer applicable. As such, one skilled in the art would not be motivated to eliminate the trusted third party when using the Woo-Lam protocol. *See In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) (holding that a *prima facie* case is not made out if

the combination of references would change the basic principle under which the reference was designed to operate).

Contrary to the position taken by the Patent Office, the Encrypted Key Protocol does not provide any motivation or suggestion to remove the trusted third party in the Woo-Lam protocol. In the Encrypted Key Protocol, the members already have a symmetric key P between them. With this key, they can communicate securely with each other without the need for a trusted third party. By setting up the symmetric key P (a shared secret key) between themselves, they have already set up their trust relationship. Since this prior trust relationship does not exist with the Woo-Lam protocol, one skilled in the art would not be motivated to eliminate the trusted third party in favor of having an unknown entity (i.e., the member) generate the session key.

B.   *The Prior Art Does Not Teach or Suggest All the Claim Limitations.*

To establish a *prima facie* case of obviousness, all the claim limitations must be taught or suggested in the prior art. In this case, none of the references cited by the Patent Office disclose or suggest, either alone or in combination, an authentication process where the key exchange request from the member to the service provider includes the member's public key.

The Patent Office acknowledges that neither Ginzboorg nor Schneier discloses the transmission of the member's public key to the service provider. Instead, the Patent Office relies on Walker for this feature. However, Walker does not disclose the process of sending of a key exchange request message from the *__member__* to the service provider, which includes the *__member's public key__*. Walker is directed to a cryptography scheme wherein the public key of one of the parties is encrypted by the private key of a trusted third party and sent to the other party by a *__digital certificate__*.

Consider the independent claims. Claims 82, 96, 103, 109 and 113 each recite formatting a "key exchange request message" at a "*__member__*," the "key exchange request message" having a "*__public key__*" of the "*__member__*," and sending the "key exchange request message" from the "*__member__*" to the "*__service provider__*." (emphasis added). Accordingly, the combination of Ginzboorg, Schneier, and Walker is legally insufficient to establish a *prima facie* case of obviousness.

Claims 83-95, 97-102, 104-108, 110-112, and 114-116 are either dependent from claim 82, 96, 103, 109 or 113, and therefore, incorporate all the limitations of the claim from which they respectively depend. Accordingly, these claims are also allowable for the same reasons set

forth hereinbefore, as well as the additional limitations cited therein. These additional limitations will not be addressed at this time because the Patent Office has not established a *prima facie* case of obviousness against the independent claims.

Objection to Drawings

The Patent Office has objected to the drawings for lack of certain labels. Proposed drawing corrections adding such labels were submitted on May 27, 2003 in accordance with MPEP § 608.02(v), and accompanied by a separate letter to the Official Draftsperson pursuant to MPEP § 608.02(r). The Examiner's comment in the pending Office action to the effect that "[n]umbers do not count as labels" strongly suggests that the Examiner has not reviewed Applicant's proposed drawing corrections. Accordingly, such action is respectfully requested. A copy of the proposed drawing corrections is attached hereto as Exhibit A for the Examiner's convenience. Formal drawings incorporating the proposed corrections will be filed after a Notice of Allowance is received.

Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested. Should any issues remain which the Examiner believes could be resolved in a telephone interview, the Examiner is requested to telephone Applicant's undersigned attorney.

Respectfully submitted,

Craig A. Gelfound
Registration No. 41,032

McDermott Will & Emery LLP
2049 Century Park East , 34th Floor
Los Angeles, CA 90067
Telephone: (310) 277-4110
Fax: (310) 277-4730

Date: September 24, 2004
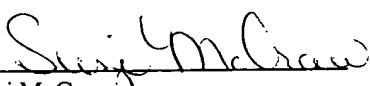
PATENT
064808-0011

Applicant:	Jay C. Chen
Serial No.:	09/456,794
Filed :	December 8, 1999
Title:	A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTION
Examiner:	Meislahn, Douglas
Group/Div.:	2132

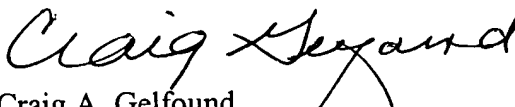## LETTER TO OFFICIAL DRAFTSPERSON

Mail Stop PGPUB Drawings
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

Pursuant to MPEP § 608.02(r), applicant submits herewith two (2) sheets of proposed drawing corrections, showing FIG. 2 and FIG 12 marked in red ink. Approval of these drawing corrections is respectfully requested.

Respectfully submitted,

Craig A. Gelfound
Registration No. 41,032

Date: **May 27, 2003**

MCDERMOTT, WILL & EMERY
2049 Century Park East, 34th Floor
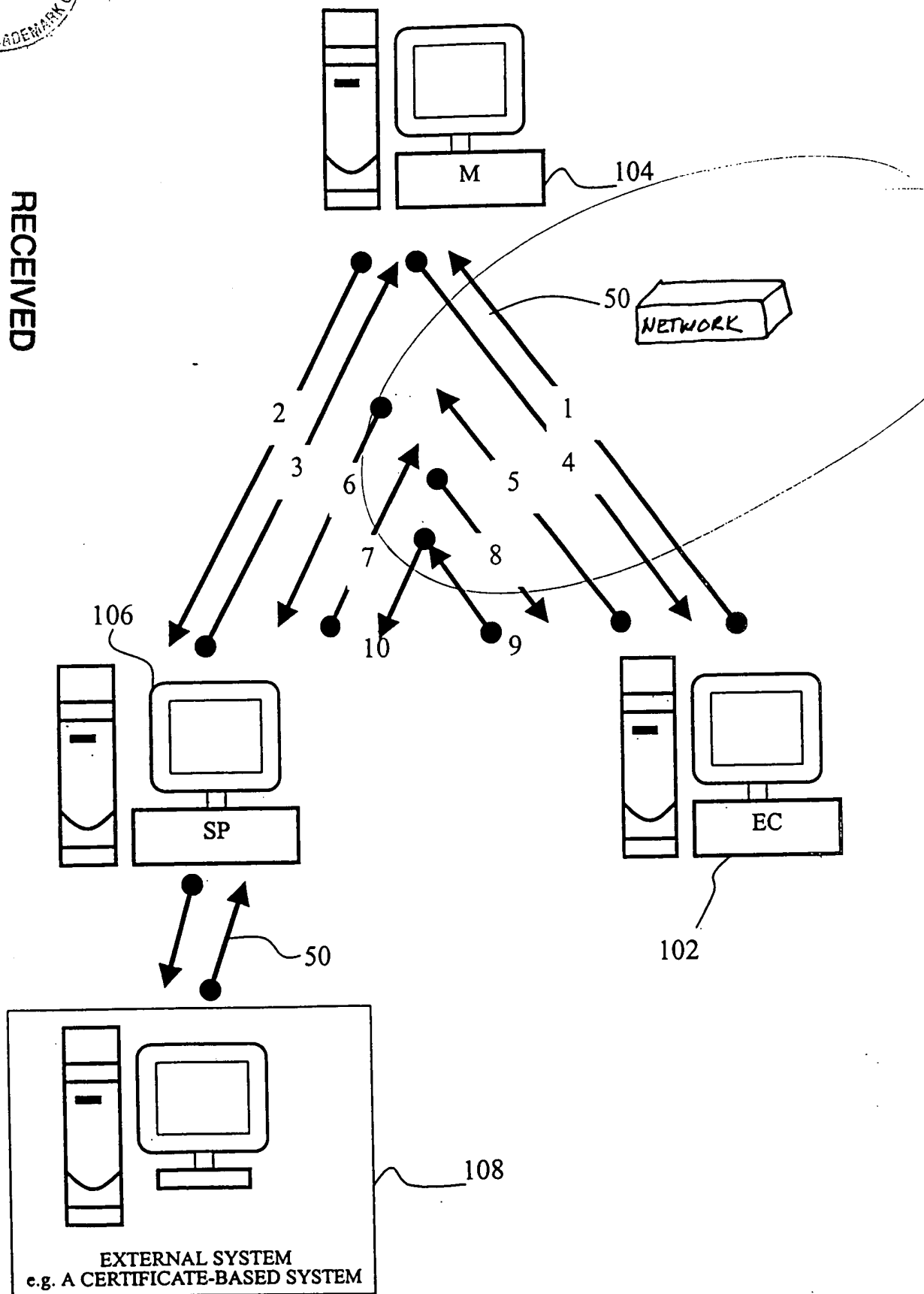Los Angeles, CA 90067
(310) 277-4110
Facsimile: (310) 277-4730

LAS99 1292557-1.064841.0011

FIG. 2

50 NETWORK

104

M

2

3

6

7

10

8

9

5

4

1

50

106

SP

EC

102

108

EXTERNAL SYSTEM
e.g. A CERTIFICATE-BASED SYSTEM

FIG. 12